10 May, 2022

Re: Impact of client side scanning on end-to-end encryption and human rights

Dear Commissioner Ylva Johansson

CC: Commissioner Didier Reynders

Access Now calls on the European Commission to refrain from including technical measures on client side scanning in upcoming legislative proposals due to their negative impact on end-to-end encryption and human rights.

Client side scanning (CSS), or any process implemented to scan content on the device before it can be shared or uploaded, is fundamentally at odds with the promise of end-to-end encryption (E2EE) and undermines the integrity of secure communications. Encryption must be guaranteed at rest and in transit. With end-to-end encryption, only the sender and the intended recipient(s) can view, access, or infer content. In circumventing E2EE, client side scanning enables third parties to discern the contents of any text message or media file. This undermines the rights to privacy, data protection, security and free expression, and violates human rights.

Protecting encryption is a long-standing and repeated commitment of the European Commission, Parliament and Council. In 2020, the Council of the European Union Resolution on Encryption noted the increased use of E2EE as well as the positive impact encryption has on society:

> *"In today's world, encryption technology is increasingly used in all areas of public and private life. It is a means to protect individuals, civil society, critical infrastructures, media and journalists, industry and governments by ensuring the privacy, confidentiality, data integrity and availability of communications and personal data: it is evident that all parties benefit from encryption technology."*

In discussing the need for authorities to be able to access content, including encrypted content, the Council reaffirmed that potential technical solutions would have to be comply with the principles of "proportionality, necessity and judicial oversight under (...) domestic legislation, while respecting common European values and upholding fundamental rights and preserving the advantages of encryption." This would not be the case of measures mandating mass client side scanning which are

inherently in contravention of the principles of necessity and proportionality that must govern any form of communications surveillance and are guaranteed under the EU Charter of Fundamental Rights. Furthermore, even if the database is initially used to identify certain types of content, once the mechanism is in place, it could be repurposed and misused to access other types of content on the device.

In addition to issues of legality, we note that there are several reliability issues with the use of client side scanning:

- In order to identify specific material, CSS would entail processing information from a database of such specific content to look for matches on the device against which content is scanned.
    - This would create security vulnerabilities that adversaries can exploit by manipulating the digital fingerprints in the database, thereby putting users at risk.
    - Machine learning parameters, artificial intelligence, and other automated filtering tools, are prone to errors. They have a history of classifying content incorrectly, resulting inevitably in a chilling effect on free expression and privacy.
- Research shows that client scanning methods are susceptible to reporting false positives. In perceptual hashing, it is not mathematically infeasible for two files to generate the same hash. In machine learning, innocuous files can be manipulated to create false alarms and equally, problematic content can be modified to evade detection.

Any measure failing to meet the principles of necessity and proportionality would harm the rule of law and undermine EU fundamental rights, including victims' rights. Considering the impact of client side scanning on end-to-end encryption and human rights, we call on the European Commission to move away from mandating this technique in any future legislation.

Sincerely,

Access Now